ABSTRACT

An information provider encrypts a content by a first encryption key so as to generate an encrypted content and encrypts a first encryption key corresponding to the first encryption key by a second encryption key so as to generated key information. The information provider provides the encrypted content and the encrypted key information in the form of a recording medium or the like to an information receiver. Moreover, the information provider has information for generating a second decryption key corresponding to the second encryption key in advance, uses it to acquire the first decryption key, and furthermore can decrypt and play back the content by using the first decryption key. The first decryption key and the second decryption key are distributed to the information receiver according to a key management method utilizing a tree structure in which an information receiver is allocated to a leaf. Here, the tree structure is divided into a plurality of hierarchies so as to define a plurality of partial trees and key information is allocated on the partial tree basis, thereby reducing the information amount of the key information to be held by the information receiver.